Remarks

At present applicants' claim 1 stands rejected under 35 U.S.C. § 102 based upon the article "Handbook of Applied Cryptography" by Menezes et al. In light of the comments presented below, this rejection is respectfully but strenuously traversed.

As a matter of formality, it is noted that the request for reversing the rejection is not being made for any reason associated with the change being made to applicants' claim 1 herein. With respect to this change, it is noted that this is solely directed to a minor typographical error. Accordingly, the claim amendment herein forms no basis for applicants arguing for the reversal of the rejection.

With respect to the rejection of applicants' claim 1, it is first noted that a rejection under 35 U.S.C. § 102 is a narrow ground of rejection. It requires each and every claim element to be found within the four corners of a single-cited document.

However, in the present rejection, it is noted that not only are the claim elements not found, it is further noted that the teachings of the documents cited by the Examiner do not in any way teach, disclose or suggest the innovation of a checksum.

The only item of substance that is common between applicants' claim 1 and the article by Menezes et al. is that they both relate to Montgomery's Multiplication Method employed for modular multiplication. Applicants' invention is however not specifically directed to a method for carrying out modular multiplication. Rather, as the first words of applicants' claim 1 recite, it is directed to "A method for checksum generation and utilization." The concept of a checksum is nowhere taught, disclosed or suggested in the art cited by the Examiner. In particular, even though the art cited does describe two-phase modular multiplication methods, the art cited does not teach, disclose or

suggest accumulating over the various cycles of the multiplication process certain sums modulo *R-1*. Likewise, the art does not teach, disclose or suggest comparing in any stage of the modulo multiplication process the accumulated sum of the Z_i with the expression $A_i B_i + N_i Y_i$, where all of the variables represent accumulated modulo *R-1* sums.

In particular, it is noted that applicants' claimed process provides for checksum generation "on the fly." Because a Montgomery Multiplication, or similar multicycle modulo multiplication which does not require a division operation, can take many cycles, it would be very useful to know whether or not there has been a hardware error during any one of these cycles, particularly an early cycle. This is a concept that does not appear to be present or appreciated in any of the art cited by the Examiner. Accordingly, for this reason and for all of the reasons indicated above, it is clear that applicants' claim 1 is not rejectable under 35 U.S.C. § 102 based upon the art cited by the Examiner. It is therefore respectfully requested that this rejection be withdrawn.

No amendment made was related to the statutory requirements of patentability unless expressly stated herein. No amendment made was for the purpose of narrowing the scope of any claim, unless applicants have argued herein that such amendment was made to distinguish over a particular cited document or combination of documents.

It is noted that the present response does not require the payment of any additional fees. It is further noted that the present response is one based on a non-final office action and accordingly, the amendments being made herein are being made as of right.

Accordingly, it is now seen that all of the applicants' claims are in condition for allowance. Therefore, early notification of the allowability of applicants' claims is earnestly solicited. Furthermore, if there are any other matters which the Examiner feels

could be expeditiously considered and which would forward the prosecution of the instant application, applicants' attorney wishes to indicate his willingness to engage in any telephonic communication in furtherance of this objective. Accordingly, applicants' attorney may be reached for this purpose at the numbers provided below.

Respectfully Submitted,

Oct. 22, 2004
Date

Lawrence D. Cutter
LAWRENCE D. CUTTER, Senior Attorney
Reg. No. 28,501

IBM Corporation, IP Law Dept.
2455 South Rd., M/S P386
Poughkeepsie, NY 12601

Phone: (845) 433-1172
FAX: (845) 432-9786
EMAIL: cutter@us.ibm.com